5.3 The Little Theorem

Note Title 5/9/2005

1. Use Fermat's Theorem to verify $17 \mid (11^{104}+1)$

Since $17 \nmid 11$, $11^{16} \equiv 1 \pmod{17}$ (Fermat's Th.)

$\therefore (11^{16})^6 = 11^{96} \equiv 1 \pmod{17}$

But $121 = 11^2$ and $7 \cdot 17 = 119 = 121 - 2$

$\therefore 11^2 \equiv 2 \pmod{17}$

$\therefore 11^8 \equiv 2^4 = 16 \pmod{17}$

$\therefore 11^{96} \cdot 11^8 \equiv 16 \pmod{17}$

$11^{104} \equiv 16 \pmod{17}$

But $16 \equiv -1 \pmod{17}$

$\therefore 11^{104} \equiv -1 \pmod{17} \Rightarrow 17 \mid 11^{104}+1$

2. (a). If $\gcd(a, 35) = 1$, show $a^{12} \equiv 1 \pmod{35}$

Since $35 = 7 \cdot 5$, Then $\gcd(a, 7) = 1$, $\gcd(a, 5) = 1$

$\therefore$ By Fermat's Theorem,

$$a^6 \equiv 1 \pmod 7 \text{ and } a^4 \equiv 1 \pmod 5$$

$\therefore a^{12} = a^6 \cdot a^6 \equiv 1 \pmod 7$, $(a^4)^3 = a^{12} \equiv 1^3 \pmod 5$

Since $\gcd(5, 7) = 1$, by corollary 2, section 2.2,

$35 \mid a^{12} - 1 \Rightarrow a^{12} \equiv 1 \pmod{35}$

(b). If $\gcd(a, 42)=1$, show $168 = 3\cdot 7\cdot 8$ divides a^6-1

Since $42 = 7\cdot 3\cdot 2$, $\gcd(a,7) = \gcd(a,3) = \gcd(a,2) = 1$

By Fermat's Th.,

$$a^6 \equiv 1 \pmod 7,\quad a^2 \equiv 1 \pmod 3,\quad a \equiv 1 \pmod 2$$

But $a^2 \equiv 1 \pmod 3 \Rightarrow a^6 = (a^2)^3 \equiv 1^3 = 1 \pmod 3$, so

$a^6 \equiv 1 \pmod 3$

Also, $a^6-1 = (a-1)(a^5+a^4+a^3+a^2+a+1)$

$= (a-1)[a^3(a^2+a+1) + a^2+a+1]$

$= (a-1)(a^3+1)(a^2+a+1)$

$= (a-1)(a+1)(a^2-a+1)(a^2+a+1)$

Assume $|a|>1$. Since a is odd,

if $a>0$, Then Then $a \geq 3$, so $2 \mid a-1$ and $4 \mid a+1$, $\therefore 8 \mid a^6-1$

if $a<0$, Then $a \leq -3$ so $4 \mid a-1$ and $2 \mid a+1$, so $8 \mid a^6-1$.

Since $7 \mid a^6-1$, $3 \mid a^6-1$, and $8 \mid a^6-1$, and $3, 7, 8$ are relatively prime, Then

$3\cdot 7\cdot 8 = 168 \mid a^6-1$

(c). If $\gcd(a, 133) = \gcd(6, 133) = 1$, show $133 \mid a^{18} - 6^{18}$

$133 = 7\cdot 19$. $\therefore \gcd(a, 19) = \gcd(6, 19) = 1$

By Fermat's Th.,

$$a^{18} \equiv 1 \pmod{19},\quad 6^{18} \equiv 1 \pmod{19}$$

$\therefore a^{18} - b^{18} \equiv 1 - 1 = 0 \pmod{19}$, $\therefore 19 \mid a^{18} - b^{18}$

Also, since $\gcd(a, 7) = \gcd(b, 7) = 1$, by Fermat's Th.,

$$a^6 \equiv 1 \pmod 7,\quad b^6 \equiv 1 \pmod 7$$

$\therefore a^6 - b^6 \equiv 0 \pmod 7$, $\therefore 7 \mid a^6 - b^6$

Since $a^{18} - b^{18} = (a^6)^3 - (b^6)^3 =$

$(a^6 - b^6)((a^6)^2 + a^6 b^6 + (b^6)^2)$, Then $7 \mid a^{18} - b^{18}$

$\therefore 7 \cdot 19 = 133 \mid a^{18} - b^{18}$

3. From Fermat's Th., show for any integer $n \geq 0$, $13 \mid 11^{12n+6} + 1$

Since $13 \nmid 11$, $11^{12} \equiv 1 \pmod{13}$ by Fermat's Th.

$\therefore 11^{12n} \equiv 1^n = 1 \pmod{13}$.

But $11^2 = 121$ and $9 \cdot 13 = 117$. $\therefore 11^2 \equiv 4 \pmod{13}$

$\therefore 11^6 \equiv 4^3 = 64 \pmod{13}$. $\therefore 11^6 \equiv 64 - 13 \cdot 5 = -1 \pmod{13}$

$\therefore 11^{12n} \cdot 11^6 \equiv 1 \cdot (-1) \pmod{13}$, or $11^{12n+6} \equiv -1 \pmod{13}$

$\therefore 13 \mid 11^{12n+6} + 1$

4. Derive each congruence

(a). $a^{21} \equiv a \pmod{15}$ for all a.

$a^5 \equiv a \pmod 5$ by Fermat's Th.
$\therefore (a^5)^4 \equiv a^4 \pmod 5$, or $a^{20} \equiv a^4 \pmod 5$
$\therefore a^{21} \equiv a^5 \equiv a \pmod 5$

Also, $a^3 \equiv a \pmod 3$, $\therefore a^{21} \equiv a^7 \pmod 3$,
and $(a^3)^2 \equiv a^2 \pmod 3$, or $a^6 \equiv a^2 \pmod 3$
$\therefore a^7 \equiv a^3 \equiv a \pmod 3$. $\therefore a^{21} \equiv a \pmod 3$

$\therefore 5 \mid a^{21}-a$ and $3 \mid a^{21}-a$, $\therefore 3\cdot 5 \mid a^{21}-a$,
$\therefore a^{21} \equiv a \pmod{15}$

(b) $a^7 \equiv a \pmod{42}$ for all a

$42 = 7\cdot 3\cdot 2$. By Fermat's Th., $a^7 \equiv a \pmod 7$
Also, $a^3 \equiv a \pmod 3$, so $a^6 \equiv a^2 \pmod 3$,
$\therefore a^7 \equiv a^3 \equiv a \pmod 3$
Also, $a^2 \equiv a \pmod 2$, $\therefore a^3 \equiv a^2 \equiv a \pmod 2$
$\therefore (a^2)^3 \equiv a^3 \equiv a \pmod 2$. $\therefore a^6 \equiv a \pmod 2$
$\therefore a^7 \equiv a^2 \equiv a \pmod 2$
$\therefore 7 \mid a^7-a$, $3 \mid a^7-a$, $2 \mid a^7-a$. $\therefore a^7 \equiv a \pmod{7\cdot 3\cdot 2}$

(c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.

By Fermat's Th., $a^{13} \equiv a \pmod{13}$

Also, $a^7 \equiv a \pmod 7$. $\therefore a^7 \cdot a^6 \equiv a \cdot a^6 \pmod 7$,

so $a^{13} \equiv a^7 \equiv a \pmod 7$

Also, $a^3 \equiv a \pmod 3$, and $\therefore a^4 \equiv a^2 \pmod 3$

$\therefore (a^3)^4 \equiv a^4 \equiv a^2 \pmod 3$, or $a^{12} \equiv a^2 \pmod 3$

$\therefore a^{13} \equiv a^{12} \cdot a \equiv a^2 \cdot a = a^3 \equiv a \pmod 3$

$\therefore 3 \mid a^{13} - a$, $7 \mid a^{13} - a$, and $13 \mid a^{13} - a$.

$\therefore a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ by Corollary 2, sec. 2.2

(d). $a^9 \equiv a \pmod{30}$ for all a.

$30 = 5 \cdot 3 \cdot 2$. Using Fermat's Th.,

$a^5 \equiv a \pmod 5$. $\therefore a^9 = a^5 \cdot a^4 \equiv a \cdot a^4 = a^5 \equiv a$

$\therefore a^9 \equiv a \pmod 5$

$a^3 \equiv a \pmod 3$ $\therefore (a^3)^3 \equiv a^3 \equiv a \pmod 3$

$\therefore a^9 \equiv a \pmod 3$

$a^2 \equiv a \pmod 2$. $\therefore$ $a^8 = (a^2)^4 \equiv a^4 \pmod 2$,

$a^4 = (a^2)^2 \equiv a^2 \equiv a \pmod 2$. $\therefore a^8 \equiv a \pmod 2$

$\therefore a^9 = a^8 \cdot a \equiv a \cdot a = a^2 \equiv a \pmod 2$

$\therefore 5 \mid a^9 - a$, $3 \mid a^9 - a$, and $2 \mid a^9 - a$, so

$a^9 \equiv a \pmod{5 \cdot 3 \cdot 2}$

5. If $\gcd(a,30)=1$, show that 60 divides a^4+59

$\gcd(a,30)=1 \Rightarrow \gcd(a,2)=\gcd(a,3)=\gcd(a,5)=1$

Also, $\gcd(a,4)=\gcd(a,2^2)=1$

$60=2^2\cdot 3\cdot 5$. $60 \mid a^4+59$ is the same as

$a^4 \equiv -59 \pmod{60}$, or $a^4 \equiv 1 \pmod{60}$

$\gcd(a,5)=1 \Rightarrow a^4 \equiv 1 \pmod{5}$ by Fermat's Th.

$\gcd(a,3)=1 \Rightarrow a^2 \equiv 1 \pmod{3}$. $\therefore a^4 \equiv 1 \pmod{3}$

$\gcd(a,2)=1 \Rightarrow a \equiv 1 \pmod{2}$, $\therefore a^2 \equiv 1 \pmod{2}$

$\therefore a^2 \equiv 1-2 = -1 \pmod{2}$

$\therefore 2 \mid a^2-1$, $2 \mid a^2+1$, $\therefore 4 \mid (a^2+1)(a^2-1) = a^4-1$

$\therefore 5 \mid a^4-1$, $3 \mid a^4-1$, $4 \mid a^4-1$, and

$\gcd(5,a)=\gcd(3,a)=\gcd(4,a)=1$

$\therefore$ By corollary 2, sec. 2.2, $60 \mid a^4-1$

$\therefore a^4 \equiv 1 \pmod{60}$, $a^4 \equiv 1-60 = -59 \pmod{60}$

$\therefore 60 \mid a^4+59$

6. (a). Find the units digit of 3^{100} using Fermat's Th.

We need something mod 10. $10 = 5 \cdot 2$

By Fermat's Th, $3^4 \equiv 1 \pmod 5$

$\therefore (3^4)^{25} = 3^{100} \equiv 1 \pmod 5$

Also, $3 \equiv 1 \pmod 2$. $\therefore 3^{100} \equiv 1 \pmod 2$

$\therefore 5 \mid 3^{100} - 1$ and $2 \mid 3^{100} - 1$.

$\therefore 5 \cdot 2 \mid 3^{100} - 1$ by corollary 2, sec. 2.2

$\therefore 3^{100} \equiv 1 \pmod{10}$

$\therefore$ units digit of 3^{100} is 1.

(b). For any integer a, verify that a^5 and a have same units digit.

By Fermat's Th., $a^5 \equiv a \pmod 5$

Also, $a^2 \equiv a \pmod 2$, $\therefore a^4 \equiv a^2 \equiv a \pmod 2$,

so $a^5 = a^4 \cdot a \equiv a \cdot a = a^2 \equiv a \pmod 2$

$\therefore 5 \mid a^5 - a$ and $2 \mid a^5 - a$. $\therefore 10 \mid a^5 - a$

$\therefore a^5 \equiv a \pmod{10}$ Let $0 \le r < 10$

$\therefore a^5 - r \equiv a - r \pmod{10}$

$\therefore a^5 - r \equiv 0 \pmod{10} \Leftrightarrow a - r \equiv 0 \pmod{10}$

$\therefore$ units digit is the same.

7. If $7 \nmid a$, prove either $7 \mid a^3+1$ or $7 \mid a^3-1$

Pf: By Fermat's Th., $a^6 \equiv 1 \pmod 7$

$\therefore 7 \mid a^6 - 1$. But $a^6 - 1 = (a^3+1)(a^3-1)$

Suppose $7 \nmid a^3+1$. $\therefore \gcd(7, a^3+1) = 1$, and so by Euclid's lemma, $7 \mid a^3 - 1$.

8. Prove

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

Pf: $1835 = 7 \cdot 262 + 1 \quad \therefore 1835 \equiv 1 \pmod 7$

$\therefore 1835^{1910} \equiv 1 \pmod 7$

$1986 = 7 \cdot 283 + 5 \quad \therefore 1986 \equiv 5 \pmod 7$

Note also $5^3 = 125 = 126 - 1$, and

$126 = 7 \cdot 18 \quad \therefore 5^3 \equiv -1 \pmod 7$

$2061 = 3 \cdot 687$

$\therefore 1986^{2061} \equiv 5^{2061} = (5^3)^{687} \equiv -1^{687} \pmod 7$

$\therefore 1986^{2061} \equiv -1^{687} = -1 \pmod 7$

$\therefore 1835^{1910} + 1986^{2061} \equiv 1 + (-1) = 0 \pmod 7$

9. (a) Let p be prime, $\gcd(a, p) = 1$. Use Fermat's Th. to verify that $x \equiv a^{p-2} b \pmod p$ is a solution to $ax \equiv b \pmod p$.

Pf: $ax \equiv b \pmod p \Rightarrow ax \cdot a^{p-2} \equiv b \cdot a^{p-2} \pmod p$

$\Rightarrow x a^{p-1} \equiv b a^{p-2} \pmod p$

But $a^{p-1} \equiv 1 \pmod p$ by Fermat's Th.

$\therefore x a^{p-1} \equiv x \pmod p$.

$\therefore x \equiv x a^{p-1} \equiv b a^{p-2} \pmod p$

$\therefore ax \equiv b \pmod p \Rightarrow x \equiv b a^{p-2} \pmod p$

(b) $2x \equiv 1 \pmod{31} \Rightarrow x \equiv 2^{31-2} = 2^{29} \pmod{31}$

But $2^5 = 32 = 31 + 1$, $\therefore 2^5 \equiv 1 \pmod{31}$

$\therefore (2^5)^5 = 2^{25} \equiv 1 \pmod{31}$.

$\therefore 2^{29} = 2^{25} \cdot 2^4 \equiv 2^4 = 16 \pmod{31}$

$\therefore 2x \equiv 1 \pmod{31} \Rightarrow \underline{x \equiv 16 \pmod{31}}$

$6x \equiv 5 \pmod{11} \Rightarrow x \equiv 5 \cdot 6^{11-2} = 5 \cdot 6^9 \pmod{11}$

But $6^2 = 36 = 33 + 3$. $\therefore 6^2 \equiv 3 \pmod{11}$

$\therefore 6^9 = (6^2)^4 \cdot 6 \equiv 3^4 \cdot 6 \pmod{11}$

$3^4 = 81 = 7 \cdot 11 + 4 \quad \therefore 3^4 \cdot 6 \equiv 4 \cdot 6 \pmod{11}$

$\therefore x \equiv 5 \cdot 6^9 \equiv 5 \cdot (4 \cdot 6) = 120 \equiv 10 \pmod{11}$

$\therefore \underline{x \equiv 10 \pmod{11}}$

$3x \equiv 17 \pmod{29} \Rightarrow x \equiv 17 \cdot 3^{29-2} \pmod{29}$

$3^3 = 27, \therefore 3^3 \equiv -2 \pmod{29}$

$\therefore 3^{27} \equiv (-2)^9, (-2)^5 = -32 \equiv -3 \pmod{29}$

$\therefore 3^{27} \equiv (-2)^9 = (-2)^5 \cdot (-2)^4 \equiv (-3)(16) = -48$

$\therefore 3^{27} \equiv -48 \equiv -48 + 58 = 10 \pmod{29}$

$\therefore 17 \cdot 3^{27} \equiv 17 \cdot 10 = 170 = 5 \cdot 29 + 25 \pmod{29}$

$\therefore \underline{x \equiv 25 \pmod{29}}$

10. Assume $p \nmid a$, $p \nmid b$, p prime

(a). If $a^p \equiv b^p \pmod{p}$, Then $a \equiv b \pmod{p}$

Pf: $a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$ for any integers a, b.

$\therefore a \equiv a^p \equiv b^p \equiv b \pmod{p}$.

(b) If $a^p \equiv b^p \pmod{p}$, Then $a^p \equiv b^p \pmod{p^2}$

By (a), $a = b + pk$, some k.

$\therefore a^p - b^p = (b+pk)^p - b^p$

$= b^p + \sum_{i=1}^{p} \binom{p}{i} b^{p-i} (pk)^i - b^p$

$= \sum_{i=1}^{p} \frac{p!}{i!(p-i)!} b^{p-i} (pk)^i$

Clearly, when $i \geq 2$, each term is divisible by p^2, since $(pk)^i$ has at least p^2 in the term.

$\therefore$ Look at $i=1$ term: $\frac{p!}{1!(p-1)!} b^{p-1} \cdot pk$

$= p \cdot b^{p-1} \cdot pk = p^2 k b^{p-1}$. So This is also divisible by p^2.

$\therefore a^p - b^p$ is divisible by p^2.

11. Use Fermat's Th. to prove that if p is an odd prime,

(a) $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$

Pf: Since p is prime ≥ 3, then $p \nmid a$ if $a < p$.
$\therefore$ By Fermat's Th., $a^{p-1} \equiv 1 \pmod{p}$.
There are $p-1$ terms in $1^{p-1} + 2^{p-1} + \dots (p-1)^{p-1}$

$\therefore 1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv (p-1)\cdot 1 \pmod{p}$
$(p-1)\cdot 1 = p-1$. Since $p \equiv 0 \pmod{p}$,
$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$

Note: it's true even if $p=2$

(b) $1^p + 2^p + \dots + (p-1)^p \equiv 0 \pmod{p}$

Pf: By corollary to Fermat's Th., $a^p \equiv a \pmod{p}$
$\therefore 1^p + 2^p + \dots + (p-1)^p \equiv 1 + 2 + \dots + (p-1) \pmod{p}$

Since $1 + 2 + \dots + n = n(n+1)/2$,
$1 + 2 + \dots + (p-1) = (p-1)(p-1+1)/2 = p(p-1)/2$
As p is an odd prime, $p-1$ is even, so
$p-1 = 2k$, some k.

$\therefore 1+2+\cdots+(p-1) = pk$, some k.

$\therefore 1^p + 2^p + \cdots + (p-1)^p \equiv pk \equiv 0 \pmod{p}$

12. Prove that if p is an odd prime, k an integer s.t. $1 \le k \le p-1$, then $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$

Pf: $\binom{p-1}{k} = \dfrac{(p-1)!}{k!\,(p-k-1)!} = \dfrac{(p-1)(p-2)\cdots(p-k)}{k!}$

$\therefore k!\binom{p-1}{k} = (p-1)(p-2)\cdots(p-k)$

But $p-j \equiv -j \pmod{p}$

$\therefore (p-1)(p-2)\cdots(p-k) \equiv (-1)(-2)\cdots(-k) \pmod{p}$

$(-1)(-2)\cdots(-k) = (-1)^k k!$

$\therefore k!\binom{p-1}{k} \equiv (-1)^k k! \pmod{p}$

Since $p-1 \ge k$, $p > k$, $\therefore p \nmid 1, 2, 3, \ldots, k$
$\therefore \gcd(p, a) = 1$, $1 \le a \le k$. $\therefore$ By Corollary 1, sec. 4.2,
$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$

13. If p, q are distinct odd primes s.t. $p-1 \mid q-1$, and if $\gcd(a, pq) = 1$, show $a^{q-1} \equiv 1 \pmod{pq}$

Pf: $\gcd(a, pq) = 1 \Rightarrow \gcd(a, p) = \gcd(a, q) = 1$ since p, q are distinct primes.

$\therefore a^{p-1} \equiv 1 \pmod{p}$ and $a^{q-1} \equiv 1 \pmod{q}$

Since $p-1 \mid q-1$, Then $q-1 = k(p-1)$, some k.

$\therefore a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{k(p-1)} \equiv 1 \pmod{p}$
$\Rightarrow a^{q-1} \equiv 1 \pmod{p}$

$\therefore p \mid a^{q-1} - 1$ and $q \mid a^{q-1} - 1$

$\therefore pq \mid a^{q-1} - 1$ by corollary 2, sec. 2.2

$\therefore a^{q-1} \equiv 1 \pmod{pq}$

14. If p, q are distinct primes, prove

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

Pf: By Fermat's Th., $p^{q-1} \equiv 1 \pmod{q}$
Clearly, $q \mid q^{p-1}$, so $q^{p-1} \equiv 0 \pmod{q}$

$\therefore\ p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$

Similarly, $p \mid p^{q-1}$ so $p^{q-1} \equiv 0 \pmod{p}$,

and $q^{p-1} \equiv 1 \pmod{p}$ by Fermat's Th.

$\therefore\ p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$.

$\therefore\ q \mid (p^{q-1} + q^{p-1} - 1)$ and $p \mid (p^{q-1} + q^{p-1} - 1)$,

and $\gcd(p, q) = 1$. $\therefore$ By corollary 2 sec. 2.2,

$pq \mid (p^{q-1} + q^{p-1} - 1)$

$\therefore\ p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

15. Establish the following.

(a) If $M_p = 2^p - 1$ is composite, p prime, then M_p is pseudoprime.

Pf: Must show $2^{M_p} \equiv 2 \pmod{M_p}$

Proof is much like proof to Th. 5.2.
Since $2^p - 1$ is composite, $p \neq 2$, so $p \nmid 2$.

By Fermat's Th. (The corollary), $2^p \equiv 2 \pmod{p}$

$\therefore\ 2^p - 2 = Kp$, some K

$\therefore\ 2^{M_p - 1} = 2^{2^p - 1 - 1} = 2^{2^p - 2} = 2^{Kp}$

$$\begin{aligned} \therefore\ 2^{M_p - 1} - 1 &= 2^{Kp} - 1 \\ &= (2^p - 1)(2^{p(K-1)} + 2^{p(K-2)} + \dots + 2^p + 1) \\ &= M_p\,(2^{p(K-1)} + 2^{p(K-2)} + \dots + 2^p + 1) \\ &\equiv 0 \pmod{M_p} \end{aligned}$$

$\therefore\ 2^{M_p - 1} \equiv 1 \pmod{M_p}$

$2 \cdot 2^{M_p - 1} \equiv 2 \pmod{M_p}$

$\therefore\ 2^{M_p} \equiv 2 \pmod{M_p}$

By def., M_p is a pseudoprime.

(6). Every composite number $F_n = 2^{2^n} + 1$ is a pseudoprime ($n = 0, 1, 2, \dots$).

Pf: Since $n + 1 \le 2^n$ for $n \ge 0$, Then $2^{n+1} \le 2^{2^n}$, so $2^{n+1} \mid 2^{2^n}$

$\therefore$ By problem #21, sec. 2-2,

$(2^{2^{n+1}}-1) \mid (2^{2^{2^n}}-1)$, or $(2^{2^{n+1}}-1) \mid (2^{F_n-1}-1)$ [1]

But $2^{2^{n+1}} = 2^{2\cdot 2^n} = 2^{(2^n)2} = (2^{2^n})^2$

$\therefore 2^{2^{n+1}}-1 = (2^{2^n})^2-1 = (2^{2^n}+1)(2^{2^n}-1)$

$= (F_n)(2^{2^n}-1)$ [2]

$\therefore$ From [2], $F_n \mid (2^{2^{n+1}}-1)$ [3]

$\therefore$ From [1] and [3], $F_n \mid (2^{F_n-1}-1)$

$\therefore F_n \mid 2(2^{F_n-1}-1) = 2^{F_n}-2$

$\therefore F_n$ is pseudoprime (whenever F_n is composite).

16. Confirm the following are absolute pseudoprimes

(a). $1105 = 5\cdot 13\cdot 17$. Let a be any integer

If $1105 \nmid a$, Then $5 \nmid a$, $13 \nmid a$, $17 \nmid a$

$\therefore$ By Fermat's Th.,

$a^4 \equiv 1 \pmod 5$, $a^{12} \equiv 1 \pmod{13}$, $a^{16} \equiv 1 \pmod{17}$

$\therefore a^{1104} = (a^4)^{276} \equiv 1 \pmod 5$

$a^{1104} = (a^{12})^{92} \equiv 1 \pmod{13}$

$a^{1104} = (a^{16})^{69} \equiv 1 \pmod{17}$

$\therefore a^{1104} \equiv 1 \pmod{5 \cdot 13 \cdot 17}$ when $1105 \nmid a$

$\therefore a^{1105} \equiv a \pmod{1105}$ when $1105 \nmid a$

But when $1105 \mid a$, clearly $1105 \mid a^{1105} - a$

$\therefore a^{1105} \equiv a \pmod{1105}$ for all a.

(6). $2821 = 7 \cdot 13 \cdot 31$ Let a be any integer

If $2821 \nmid a$, Then $7 \nmid a$, $13 \nmid a$, $31 \nmid a$

$\therefore a^6 \equiv 1 \pmod 7$, $a^{12} \equiv 1 \pmod{13}$, $a^{30} \equiv 1 \pmod{31}$

$\therefore a^{2820} = (a^6)^{470} \equiv 1 \pmod 7$

$a^{2820} = (a^{12})^{235} \equiv 1 \pmod{13}$

$a^{2820} = (a^{30})^{94} \equiv 1 \pmod{31}$

$\therefore a^{2820} \equiv 1 \pmod{7 \cdot 13 \cdot 31}$ when $2821 \nmid a$

$\therefore a^{2821} \equiv a \pmod{2821}$ when $2821 \nmid a$

But when $2821 \mid a$, clearly $a^{2821} \equiv a \pmod{2821}$

$\therefore$ For all a, $a^{2821} \equiv a \pmod{2821}$

(c) $2465 = 5 \cdot 17 \cdot 29$ Let a be any integer

If $2465 \nmid a$, Then $5 \nmid a$, $17 \nmid a$, $29 \nmid a$

$\therefore a^4 \equiv 1 \pmod 5$, $a^{16} \equiv 1 \pmod{17}$, $a^{28} \equiv 1 \pmod{29}$

$a^{2464} = (a^4)^{616} \equiv 1 \pmod 5$

$a^{2464} = (a^{16})^{154} \equiv 1 \pmod{17}$

$a^{2464} = (a^{28})^{88} \equiv 1 \pmod{29}$

$\therefore a^{2464} \equiv 1 \pmod{5 \cdot 17 \cdot 29}$ when $2465 \nmid a$

$\therefore a^{2465} \equiv a \pmod{2465}$ when $2465 \nmid a$

But when $2465 \mid a$, clearly $a^{2465} \equiv a \pmod{2465}$

$\therefore$ For all a, $a^{2465} \equiv a \pmod{2465}$

17. Show that the smallest pseudoprime 341 is not an an absolute prime by showing $11^{341} \not\equiv 11 \pmod{341}$

$341 = 11 \cdot 31$. Suppose $11^{341} \equiv 11 \pmod{341}$

Then $11^{341} \equiv 11 \pmod{31}$. But $11^2 = 121 \equiv -3 \pmod{31}$

$\therefore 11^{2\cdot 170} \equiv (-3)^{170} \pmod{31}$

But $(-3)^9 = -19683$ and $-635 \cdot 31 = -19685$

$\therefore (-3)^9 \equiv 2 \pmod{31}$

$\therefore (-3)^{9\cdot 18} = (-3)^{162} \equiv 2^{18} \pmod{31}$

But $2^{10} = 1024 \equiv 1 \pmod{31}$ $(31 \cdot 33 = 1023)$

$2^8 = 256 = 8\cdot 31 + 8 \equiv 8 \pmod{31}$

$\therefore 2^{18} \equiv 8 \pmod{31}$

$\therefore (-3)^{162} \equiv 8 \pmod{31}$

$(-3)^4 = 81 = 2\cdot 31 + 19 \equiv 19 \pmod{31}$

$\therefore (-3)^8 \equiv 19^2 = 361 = 31\cdot 11 + 20 \equiv 20 \pmod{31}$

$\therefore (-3)^{162} \cdot (-3)^8 \equiv 8 \cdot 20 = 160 = 5\cdot 31 + 5 \equiv 5 \pmod{31}$

$\therefore 11^{340} \equiv (-3)^{170} \equiv 5 \pmod{31}$

$\therefore 11^{341} \equiv 5 \cdot 11 = 55 = 31 + 24 \equiv 24 \pmod{31}$

$\therefore 11^{341} \equiv 24 \pmod{31}$, so $11^{341} \not\equiv 11 \pmod{31}$

$\therefore$ Contradiction reached, so $11^{341} \not\equiv 11 \pmod{341}$

Note: assuming $11^{341} \equiv 11 \pmod{341} \Rightarrow 11^{341} \equiv 11 \pmod{11}$
But since $11^{10} \equiv 1 \pmod{11}$, $11^{340} \equiv 1 \pmod{11}$,
and $\therefore 11^{341} \equiv 11 \pmod{11}$. That's why
attacked problem using mod 31.

18. (a) When $n = 2p$, p an odd prime, prove $a^{n-1} \equiv a \pmod{n}$
for any integer a.

Pf: $a^{p-1} \equiv 1 \pmod{p}$ (Fermat Th.), and $a^p \equiv a \pmod{p}$

$\therefore a^p \cdot a^{p-1} = a^{2p-1} \equiv a^p \equiv a \pmod{p}$

As $2p = n$, $\therefore a^{n-1} \equiv a \pmod{p}$, so $p \mid a^{n-1} - a$.

Now, if a is even, let $a = 2x$, some x

$\therefore a^{n-1} - a = (2x)^{n-1} - 2x = 2^{n-1}x^{n-1} - 2x$
$= 2(2^{n-2}x^{n-1} - x)$

Since $n \geq 2$, Then $2 \mid a^{n-1} - a$

Suppose a is odd. Since $2p$ is even,

$n-1$ is odd. $\therefore a^{n-1}$ is odd, and
$\therefore a^{n-1} - a$ is even, so $2 \mid a^{n-1} - a$.

$\therefore$ Both 2 and p divide $a^{n-1} - a$.
Since $\gcd(2, p) = 1$, then $2p \mid a^{n-1} - a$,
so $a^{n-1} \equiv a \pmod{n}$

(6) For $n = 195 = 3 \cdot 5 \cdot 13$, verify $a^{n-2} \equiv a \pmod{n}$ for any integer a.

Pf: If $195 \mid a$, then clearly $195 \mid a^{n-2} - a$
$\therefore$ Assume $195 \nmid a$.
$\therefore 3 \nmid a$, $5 \nmid a$, $13 \nmid a$.
$\therefore$ By Fermat's Th., $a^2 \equiv 1 \pmod{3}$
$a^4 \equiv 1 \pmod{5}$
$a^{12} \equiv 1 \pmod{13}$

$\therefore a^{192} = a^{2 \cdot 96} \equiv 1 \pmod{3}$
$a^{192} = a^{4 \cdot 48} \equiv 1 \pmod{5}$
$a^{192} = a^{12 \cdot 16} \equiv 1 \pmod{13}$

$\therefore a^{192} \equiv 1 \pmod{3 \cdot 5 \cdot 13}$
$\therefore a^{193} \equiv a \pmod{n}$
$\therefore a^{n-2} \equiv a \pmod{n}$

19. Prove any integer of the form

$$n = (6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime if all three factors are prime

Pf; Let $p_1 = 6k+1$, $p_2 = 12k+1$, $p_3 = 18k+1$

Assume p_1, p_2, p_3 are prime.

$$n = (72k^2 + 18k + 1)(18k+1)$$
$$= 18 \cdot 72 k^3 + 72k^2 + 18 \cdot 18 k^2 + 18k + 18k + 1$$
$$= 36 \cdot 36 k^3 + 36 \cdot 2k^2 + 36 \cdot 9 k^2 + 36k + 1$$
$$\therefore n - 1 = 36k[36k^2 + 11k^2 + 1]$$
$$\therefore (p_1 - 1) \mid (n-1),\ (p_2 - 1) \mid (n-1),\ (p_3 - 1) \mid n-1$$

Since p_1, p_2, p_3 are distinct primes, and n is square-free (each prime of power 1), then n is absolute pseudoprime by Th. 5.3

20. Show that $561 \mid 2^{561} - 2$ and $561 \mid 3^{561} - 3$

(a). $2^2 \equiv 1 \pmod{3}$, $\therefore (2^2)^{280} = 2^{560} \equiv 1 \pmod{3}$

$2^{10} \equiv 1 \pmod{11}$ (Fermat's Th.)

$\therefore (2^{10})^{56} = 2^{560} \equiv 1 \pmod{11}$

$2^{16} \equiv 1 \pmod{17}$ (Fermat's Th.)

$\therefore (2^{16})^{35} = 2^{560} \equiv 1 \pmod{17}$

$\therefore 2^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$, and $3 \cdot 11 \cdot 17 = 561$

$\therefore 2^{560} \cdot 2 \equiv 2 \pmod{561}$, $\therefore 561 \mid 2^{561} - 2$

(b) By Fermat's Th, $3^{10} \equiv 1 \pmod{11}$, $3^{16} \equiv 1 \pmod{17}$

$\therefore 3^{560} \equiv 1 \pmod{11}$, $3^{560} \equiv 1 \pmod{17}$

$\therefore 11 \mid 3^{561} - 3$, $17 \mid 3^{561} - 3$,

$\therefore 11 \cdot 17 \mid 3^{561} - 3$. Clearly $3 \mid 3^{561} - 3$

$\therefore 3 \cdot 11 \cdot 17 \mid 3^{561} - 3$ since $\gcd(3, 11, 17) = 1$

Alternatively, $3^7 = 2187 = 4 \cdot 561 - 57$,

$\therefore 3^7 \equiv -57 \pmod{561}$

$\therefore (3^7)^{80} = 3^{560} \equiv (-57)^{80} \pmod{561}$

But $57^2 = 3249 = 6 \cdot 561 - 117$

$\therefore 57^2 \equiv (-117) \pmod{561}$, and $(57^2)^{40} = (-57)^{80}$

$$\therefore 3^{560} \equiv (-117)^{40} \pmod{561}$$

$$(-117)^2 = 13689 = 24 \cdot 561 + 225$$

$$\therefore (-117)^2 \equiv 225 \pmod{561}$$

$$\therefore 3^{560} \equiv (-117)^{40} \equiv 225^{20} \pmod{561}$$

$$225^2 = 50625 = 90 \cdot 561 + 135$$

$$\therefore 225^2 \equiv 135 \pmod{561}$$

$$\therefore 3^{560} \equiv 225^{20} \equiv 135^{10} \pmod{561}$$

$$135^2 = 18225 = 32 \cdot 561 + 273$$

$$\therefore 135^2 \equiv 273 \pmod{561}$$

$$\therefore 3^{560} \equiv 135^{10} \equiv 273^5 \pmod{561}$$

$$273^2 = 74529 = 133 \cdot 561 - 84$$

$$\therefore 273^2 \equiv -84 \pmod{561}$$

$\therefore (273)^4 \equiv (-84)^2 = 7056 = 12\cdot 561 + 324$

$\therefore 3^{560} \equiv 273^5 = 273^4 \cdot 273$
$\equiv (-324)\cdot 273 \pmod{561}$

But $-324\cdot 273 = -88452 = -157\cdot 561 - 375$

$\therefore 3^{560} \equiv (-324)\cdot 273 \equiv -375 \pmod{561}$
$\equiv 186 \pmod{561}$

$\therefore 3^{561} \equiv 3\cdot 186 = 558 \pmod{561}$

$\therefore 3^{561} + 3 \equiv 558 + 3 \equiv 0 \pmod{561}$,

$\therefore 3^{561} \equiv 3 \pmod{561}$

21. Show $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$

$1111 = 159\cdot 7 - 2 \quad \therefore 1111 \equiv -2 \pmod{7}$

$\therefore 2222 \equiv -4 \pmod{7}$, $5555 \equiv -10 \equiv -10 + 14 = 4 \pmod{7}$

$\therefore 2222^{5555} \equiv (-4)^{5555} \pmod{7}$

But $(-4)^2 = 16 \equiv 2 \pmod{7}$, $5555 = 2(2777) + 1$

$\therefore (-4)^{5555} = (-4)^{2(2777)+1} \equiv 2^{2777}\cdot(-4) \pmod{7}$

$\therefore 2222^{5555} \equiv -2^{2779} \pmod 7$

But $2^3 \equiv 1 \pmod 7$, and $3 \cdot 926 = 2778$

$\therefore (2^3)^{926} = 2^{2778} \equiv 1 \pmod 7$

$\therefore 2222^{5555} \equiv -2^{2779} = -2^{2778}(2) \equiv -2 \pmod 7$

Now $5555 \equiv 4 \pmod 7 \Rightarrow 5555^{2222} \equiv 4^{2222} \pmod 7$

$\therefore 5555^{2222} \equiv 2^{4444} \pmod 7$

and $4444 = 1481 \cdot 3 + 1$, and $2^3 \equiv 1 \pmod 7$

$\therefore 5555^{2222} \equiv (2^3)^{1481} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod 7$

$\therefore 2222^{5555} + 5555^{2222} \equiv -2 + 2 = 0 \pmod 7$

Theorem 5.3 - a more explicit proof

Let n be a composite square-free integer, say, $n = p_1 p_2 p_3 \dots p_r$, each p_i distinct.

If $(p_i - 1) \mid (n-1)$ for $i = 1, 2, \dots, r$, Then n is absolute prime.

Pf: Suppose initially a is some integer s.t.

$\gcd(a,n)=1$. $\therefore \gcd(a,p_i)=1$ for each i

Fermats Th. yields $p_i \mid a^{p_i-1}-1$

Since $(p_i-1)\mid(n-1)$, then $n-1=k(p_i-1)$, some k.

$$\therefore a^{k(p_i-1)}-1 = (a^{p_i-1}-1)(a^{(p_i-1)(k-1)}+\cdots a^{p_i-1}+1)$$

$\therefore p_i \mid a^{n-1}-1$ for all i.

$\therefore p_i \mid a^n-a$ for all i.

$\therefore$ From corollary 2, Th. 2.4 (sec. 2.2),

$n \mid a^n-a$

Now if $\gcd(a,n)\neq 1$, then let

$\gcd(a,n)=p_{j_1}p_{j_2}\cdots p_{j_s}$, where $p_{j_x}\in\{p_1,\ldots p_r\}$

Since n is square-free and composed of distinct primes, then p_{j_x} are all distinct and have exponents of 1.

Let $a' = a / p_{j_1} p_{j_2} \cdots p_{j_s}$

$\therefore a = (p_{j_1} \cdot p_{j_2} \cdot \cdots p_{j_x})(a')$ [1]

$\therefore \gcd(a', n) = 1$, and from above,

$n \mid (a')^n - a$

$\therefore n \mid (p_{j_1} \cdot p_{j_2} \cdots p_{j_x})^n (a')^n - (p_{j_1} p_{j_2} \cdots p_{j_x})(a')$

From [1] above, $(p_{j_1} p_{j_2} \cdots p_{j_x})(a') = a$

$\therefore n \mid a^n - a$ if $\gcd(a, n) \neq 1$

$\therefore n \mid a^n - a$ for all a.